Complete Weight Enumerators of Generalized Doubly-Even Self-Dual Codes

Gabriele Nebe *, H.-G. Quebbemann †, E. M. Rains ‡ and N. J. A. Sloane §

ABSTRACT For any q which is a power of 2 we describe a finite subgroup of $\mathrm{GL}_q(\mathbb{C})$ under which the complete weight enumerators of generalized doubly-even self-dual codes over $\mathbb{F}_q$ are invariant. An explicit description of the invariant ring and some applications to extremality of such codes are obtained in the case $q = 4$.

1 Introduction

In 1970 Gleason [5] described a finite complex linear group of degree q under which the complete weight enumerators of self-dual codes over $\mathbb{F}_q$ are invariant. While for odd q this group is a double or quadruple cover of $\mathrm{SL}_2(\mathbb{F}_q)$, for even $q \geq 4$ it is solvable of order $4q^2(q-1)$ (compare [6]). For even q it is only when $q = 2$ that the seemingly exceptional type of doubly-even self-dual binary codes leads to a larger group.

In this paper we study a generalization of doubly-even codes to the non-binary case which was introduced in [11]. A linear code of length n over $\mathbb{F}_q$ is called doubly-even if all of its words are annihilated by the first and the second elementary symmetric polynomials in n variables. For $q = 2$ this condition is actually equivalent to the usual one on weights modulo 4, but for $q \geq 4$ it does not restrict the Hamming weight over $\mathbb{F}_q$. (For odd q the condition just means that the code is self-orthogonal and its dual contains the all-ones word; however here we consider only characteristic 2.) Extended Reed-Solomon codes of rate $\frac{1}{2}$ are known to be examples of doubly-even self-dual codes. For $q = 4^e$ another interesting class of examples is given by the extended quadratic-residue codes of lengths divisible by 4.

* Abteilung Reine Mathematik, Universität Ulm, 89069 Ulm, Germany, nebe@mathematik.uni-ulm.de

† Fachbereich Mathematik, Universität Oldenburg, 26111 Oldenburg, Germany, quebbemann@mathematik.uni-oldenburg.de

‡ Mathematics Department, University of California Davis, Davis, CA 95616, USA, rains@math.ucdavis.edu

§ Information Sciences Research, AT&T Shannon Labs, Florham Park, NJ 07932-0971, USA, njas@research.att.com

We find (Theorems 11 and 16) that the complete weight enumerators of doubly-even self-dual codes over $\mathbb{F}_q$, $q = 2^f$, are invariants for the same type of Clifford-Weil group that for odd primes q has been discussed in [12], Section 7.9. More precisely, the group has a normal subgroup of order $4q^2$ or $8q^2$ (depending on whether f is even or odd) such that the quotient is $\mathrm{SL}_2(\mathbb{F}_q)$. Over $\mathbb{F}_4$ the invariant ring is still simple enough to be described explicitly. Namely, the subring of Frobenius-invariant elements is generated by the algebraically independent weight enumerators of the four extended quadratic-residue codes of lengths 4, 8, 12 and 20, and the complete invariant ring is a free module of rank 2 over this subring; the fifth (not Frobenius-invariant) basic generator has degree 40. In the final section we use this result to find the maximal Hamming distance of doubly-even self-dual quaternary codes up through length 24. Over the field $\mathbb{F}_4$, doubly-even codes coincide with what are called "Type II" codes in [4].

The invariant ring considered here is always generated by weight enumerators. This property holds even for Clifford-Weil groups associated with multiple weight enumerators, for which a direct proof in the binary case was given in [8]. The general case can be found in [9], where still more general types of codes are also included.

2 Doubly even codes

In this section we generalize the notion of doubly-even binary codes to arbitrary finite fields of characteristic 2 (see [11]).

Let $\mathbb{F} := \mathbb{F}_{2^f}$ denote the field with 2^f elements. A code $C \leq \mathbb{F}^n$ is an $\mathbb{F}$-linear subspace of $\mathbb{F}^n$. If $c \in \mathbb{F}^n$ then the i-th coordinate of c is denoted by c_i. The dual code to a code $C \leq \mathbb{F}^n$ is defined to be

$$C^{\perp} := \{v \in \mathbb{F}^n \mid \sum_{i=1}^{n} c_i v_i = 0 \text{ for all } c \in C\}.$$

C is called self-orthogonal if $C \subset C^{\perp}$, and self-dual if $C = C^{\perp}$.

Definition 1 *A code $C \leq \mathbb{F}^n$ is* doubly-even *if*

$$\sum_{i=1}^{n} c_i = \sum_{i<j} c_i c_j = 0$$

for all $c \in C$.

Remark 2 *An alternative definition can be obtained as follows. There is a unique unramified extension $\hat{\mathbb{F}}$ of the 2-adic integers with the property that*

$\hat{\mathbb{F}}/2\hat{\mathbb{F}} \cong \mathbb{F}$; moreover, the map $x \mapsto x^2$ induces a well-defined map $\hat{\mathbb{F}}/2\hat{\mathbb{F}} \to \hat{\mathbb{F}}/4\hat{\mathbb{F}}$, and thus a map (also written as $x \mapsto x^2$) from $\mathbb{F} \to \hat{\mathbb{F}}/4\hat{\mathbb{F}}$. The above condition is then equivalent to requiring that $\sum_i v_i^2 = 0 \in \hat{\mathbb{F}}/4\hat{\mathbb{F}}$ for all $v \in C$.

Doubly-even codes are self-orthogonal. This follows from the identity

$$\sum_{i<j}(c_i + c_i')(c_j + c_j') = \sum_{i<j} c_i c_j + \sum_{i<j} c_i' c_j' + \sum_{i=1}^{n} c_i \sum_{i=1}^{n} c_i' - \sum_{i=1}^{n} c_i c_i'.$$

Note that Hamming distances in a doubly-even code are not necessarily even:

Example 3 *Let $\omega \in \mathbb{F}_4$ be a primitive cube root of unity. Then the code $Q_4 \le \mathbb{F}_4^4$ with generator matrix*

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \omega & \omega^2 \end{pmatrix}$$

is a doubly-even self-dual code over $\mathbb{F}_4$.

Let $B = (b_1, \ldots, b_f)$ be an $\mathbb{F}_2$-basis of $\mathbb{F}$ such that $\tau(b_i b_j) = \delta_{ij}$ for all $i, j = 1, ..., f$, where τ denotes the trace of $\mathbb{F}$ over $\mathbb{F}_2$. Then B is called a self-complementary (or trace-orthogonal) basis of $\mathbb{F}$ (cf. [10], [11], [15]). Using such a basis we identify $\mathbb{F}$ with $\mathbb{F}_2^f$ and define

$$\varphi : \mathbb{F} \to \mathbb{Z}/4\mathbb{Z},\ \varphi(\sum_{i=1}^{f} a_i b_i) := \mathrm{wt}(a_1, \ldots, a_f) + 4\mathbb{Z}$$

to be the weight modulo 4. Since $\tau(b_i) = \tau(b_i^2) = 1$, we have

$$\varphi(a) + 2\mathbb{Z} = \tau(a)$$

and (considering 2τ as a map onto $2\mathbb{Z}/4\mathbb{Z}$)

$$\varphi(a + a') = \varphi(a) + \varphi(a') + 2\tau(aa')$$

for all $a, a' \in \mathbb{F}$. More generally,

$$\varphi(\sum_{i=1}^{n} c_i) = \sum_{i=1}^{n} \varphi(c_i) + 2\tau(\sum_{i<j} c_i c_j).$$

We extend φ to a quadratic function

$$\phi : \mathbb{F}^n \to \mathbb{Z}/4\mathbb{Z},\ \phi(c) := \sum_{i=1}^{n} \varphi(c_i).$$

Proposition 4 *A code $C \le \mathbb{F}^n$ is doubly-even if and only if $\phi(C) = \{0\}$.*

Proof. For $r \in \mathbb{F}, c \in \mathbb{F}^n$,

$$\phi(rc) = \varphi(\sum_{i=1}^{n} rc_i) - 2\tau(\sum_{i<j} r^2 c_i c_j).$$

This equation in particular shows that $\phi(C) = \{0\}$ if C is doubly-even. Conversely, if $\phi(C) = \{0\}$ then the same equation shows that $\tau(r \sum_{i=1}^{n} c_i) = \varphi(\sum_{i=1}^{n} rc_i) + 2\mathbb{Z} = 0$ for all $r \in \mathbb{F}$, $c \in C$. Since the trace bilinear form is non-degenerate, this implies that $\sum_{i=1}^{n} c_i = 0$ for all $c \in C$. The same equality then implies that $\tau(r^2 \sum_{i<j} c_i c_j) = 0$ for all $r \in \mathbb{F}$ and $c \in C$. The mapping $r \mapsto r^2$ is an automorphism of $\mathbb{F}$, so again the non-degeneracy of the trace bilinear form yields $\sum_{i<j} c_i c_j = 0$ for all $c \in C$. □

Corollary 5 *Let $\mathbb{F}^n$ be identified with $\mathbb{F}_2^{nf}$ via a self-complementary basis. Then a doubly-even code $C \leq \mathbb{F}^n$ becomes a doubly-even binary code $C_{\mathbb{F}_2} \leq \mathbb{F}_2^{nf}$.*

Remark 6 *Let $C \leq \mathbb{F}^n$ be a doubly-even code. Then $\mathbf{1} := (1, \ldots, 1) \in C^{\perp}$. Hence if C is self-dual then 4 divides n.*

In the following remark we use the fact that the length of a doubly-even self-dual binary code is divisible by 8.

Remark 7 *If $f \equiv 1 \pmod 2$ then the length of a doubly-even self-dual code over $\mathbb{F}$ is divisible by 8. If $f \equiv 0 \pmod 2$ then $\mathbb{F} \otimes_{\mathbb{F}_4} Q_4$ is a doubly-even self-dual code over $\mathbb{F}$ of length 4.*

More general examples of doubly-even self-dual codes are provided by extended quadratic-residue codes (see [7]). Let p be an odd prime and let ζ be a primitive p-th root of unity in an extension field $\tilde{\mathbb{F}}$ of $\mathbb{F}_2$. Let

$$g := \prod_{a \in (\mathbb{F}_p^*)^2} (X - \zeta^a) \in \tilde{\mathbb{F}}[X]$$

where a runs through the non-zero squares in $\mathbb{F}_p$. Then $g \in \mathbb{F}_4[X]$ divides $X^p - 1$, and g lies in $\mathbb{F}_2[X]$ if g is fixed under the Frobenius automorphism $z \mapsto z^2$, i.e. if 2 is a square in $\mathbb{F}_p^*$, or equivalently by quadratic reciprocity if $p \equiv \pm 1 \pmod 8$. Assuming f to be even if $p \equiv \pm 3 \pmod 8$, we define the quadratic-residue code $\mathrm{QR}(\mathbb{F}, p) \leq \mathbb{F}^p$ to be the cyclic code of length p with generator polynomial g. Then $\dim(\mathrm{QR}(\mathbb{F}, p)) = p - \deg(g) = \frac{p+1}{2}$, which is also the dimension of the extended code $\widetilde{\mathrm{QR}}(\mathbb{F}, p) \leq \mathbb{F}^{p+1}$.

From [7, pages 490, 508] together with Proposition 4 we obtain the following (the case $\mathbb{F} = \mathbb{F}_4$ was given in [4, Proposition 4.1]):

Proposition 8 *Let p be a prime, $p \equiv 3 \pmod 4$. Then the extended quadratic-*

residue code $\widetilde{\mathrm{QR}}(\mathbb{F}, p)$ is a doubly-even self-dual code.

3 Complete weight enumerators and invariant rings

In this section we define the action of a group of $\mathbb{C}$-algebra automorphisms on the polynomial ring $\mathbb{C}[x_a \mid a \in \mathbb{F}]$ such that the complete weight enumerators of doubly-even self-dual codes are invariant under this group.

Definition 9 *Let $C \leq \mathbb{F}^n$ be a code. Then*

$$\mathrm{cwe}(C) := \sum_{c \in C} \prod_{i=1}^{n} x_{c_i} \in \mathbb{C}[x_a \mid a \in \mathbb{F}]$$

is the complete weight enumerator *of C.*

For an element $r \in \mathbb{F}$ let m_r and d_r be the $\mathbb{C}$-algebra endomorphisms of $\mathbb{C}[x_a \mid a \in \mathbb{F}]$ defined by

$$m_r(x_a) := x_{ar}, \quad d_r(x_a) := i^{\varphi(ar)} x_a \quad \text{for all } a \in \mathbb{F},$$

where $i = \sqrt{-1}$ and $\varphi : \mathbb{F} \to \mathbb{Z}/4\mathbb{Z}$ is defined as above via a fixed self-complementary basis. We also have the MacWilliams transformation h defined by

$$h(x_a) := 2^{-f/2} \sum_{b \in \mathbb{F}} (-1)^{\tau(ab)} x_b \text{ for all } a \in \mathbb{F}.$$

Definition 10 *The group*

$$G_f := \langle h, m_r, d_r \mid 0 \neq r \in \mathbb{F} \rangle$$

is called the associated Clifford-Weil group.

Gleason ([5]) observed that the complete weight enumerator of a self-dual code C remains invariant under the transformations h and m_r. If C is doubly-even, then $\mathrm{cwe}(C)$ is invariant also under each d_r (Proposition 4). Therefore we have the following theorem.

Theorem 11 *The complete weight enumerator of a doubly-even self-dual code over $\mathbb{F}$ lies in the invariant ring*

$$\mathrm{Inv}(G_f) := \{p \in \mathbb{C}[x_a \mid a \in \mathbb{F}] \mid pg = p \textit{ for all } g \in G_f\}.$$

By the general theory developed in [9] one finds that a converse to Theorem 11 also holds:

Theorem 12 *The invariant ring of G_f is generated by complete weight enumerators of doubly-even self-dual codes over $\mathbb{F}$.*

In the case $f = 1$ Gleason obtained the more precise information

$$\mathrm{Inv}(G_1) = \mathbb{C}[\mathrm{cwe}(\mathcal{H}_8), \mathrm{cwe}(\mathcal{G}_{24})]$$

where $\mathcal{H}_8$ and $\mathcal{G}_{24}$ denote the extended Hamming code of length 8 and the extended Golay code of length 24 over $\mathbb{F}_2$.

In general, the Galois group

$$\Gamma_f := \mathrm{Gal}(\mathbb{F}/\mathbb{F}_2)$$

acts on $\mathrm{Inv}(G_f)$ by $\gamma(x_a) := x_{a^\gamma}$ for all $a \in \mathbb{F}, \gamma \in \Gamma_f$. Let $\mathrm{Inv}(G_f, \Gamma_f)$ denote the ring of Γ_f-invariant polynomials in $\mathrm{Inv}(G_f)$.

Theorem 13

$$\mathrm{Inv}(G_2, \Gamma_2) = \mathbb{C}[\mathrm{cwe}(Q_4), \mathrm{cwe}(Q_8), \mathrm{cwe}(Q_{12}), \mathrm{cwe}(Q_{20})]$$

where Q_{p+1} denotes the extended quadratic-residue code of length $p+1$ over $\mathbb{F}_4$ (see Proposition 8). The invariant ring of G_2 is a free module of rank 2 over $\mathrm{Inv}(G_2, \Gamma_2)$:

$$\mathrm{Inv}(G_2) = \mathrm{Inv}(G_2, \Gamma_2) \oplus \mathrm{Inv}(G_2, \Gamma_2) p_{40}$$

where p_{40} is a homogeneous polynomial of degree 40 which is not invariant under Γ_2.

Proof. Computation shows that $\langle G_2, \Gamma_2 \rangle$ is a complex reflection group of order $2^9 3 \cdot 5$ (Number 29 in [13]) and G_2 is a subgroup of index 2 with Molien series

$$\frac{1 + t^{40}}{(1 - t^4)(1 - t^8)(1 - t^{12})(1 - t^{20})}.$$

By Proposition 8 the codes Q_i ($i = 4, 8, 12, 20$) are doubly-even self-dual codes over $\mathbb{F}_4$. Their complete weight enumerators (which are Γ_2-invariant) are algebraically independent elements in the invariant ring of G_2 as one shows by an explicit computation of their Jacobi matrix. Therefore these polynomials generate the algebra $\mathrm{Inv}(G_2, \Gamma_2)$. □

By Theorem 12 we have the following corollary.

Corollary 14 *There is a doubly-even self-dual code C over $\mathbb{F}_4$ of length 40 such that $\mathrm{cwe}(C)$ is not Galois invariant.*

A code with this property was recently constructed in [2].

For $f > 2$ the following example shows that we cannot hope to find an explicit description of the invariant rings of the above type.

Example 15 *The Molien series of G_3 is N/D, where*

$$D = (1-t^8)^2(1-t^{16})^2(1-t^{24})^2(1-t^{56})(1-t^{72})$$

and $N(t) = M(t) + M(t^{-1})t^{216}$ with

$$M = 1 + 5t^{16} + 77t^{24} + 300t^{32} + 908t^{40} + 2139t^{48} + 3808t^{56} + 5864t^{64}$$

$$+8257t^{72} + 10456t^{80} + 12504t^{88} + 14294t^{96} + 15115t^{104}.$$

The Molien series of $\langle G_3, \Gamma_3 \rangle$ is $(L(t) + L(t^{-1})t^{216})/D$, where D is as above and

$$L = 1 + 3t^{16} + 29t^{24} + 100t^{32} + 298t^{40} + 707t^{48} + 1268t^{56} + 1958t^{64}$$

$$+2753t^{72} + 3482t^{80} + 4166t^{88} + 4766t^{96} + 5045t^{104}.$$

4 The structure of the Clifford-Weil groups G_f

In this section we establish the following theorem.

Theorem 16 *The structure of the Clifford-Weil groups G_f is given by*

$$G_f \cong Z.(\mathbb{F} \oplus \mathbb{F}).\,\mathrm{SL}_2(\mathbb{F})$$

where $Z \cong \mathbb{Z}/4\mathbb{Z}$ if f is even, and $Z \cong \mathbb{Z}/8\mathbb{Z}$ if f is odd.

To prove this theorem, we first construct a normal subgroup $N_f \trianglelefteq G_f$ with $N_f \cong \mathbb{Z}/4\mathbb{Z}\mathsf{Y}2_+^{1+2f}$, the central product of an extraspecial group of order 2^{1+2f} with the cyclic group of order 4. The image of the homomorphism $G_f/N_f \to \mathrm{Out}(N_f)$ is isomorphic to $\mathrm{SL}_2(\mathbb{F})$ and the kernel consists of scalar matrices only.

Let $q_r := (d_r^2)^h = hd_r^2h$ and

$$N_f := \langle d_r^2, q_r, i\,\mathrm{id} \mid r \in \mathbb{F} \rangle.$$

Using the fact that $(-1)^{\varphi(b)} = (-1)^{\tau(b)}$ for all $b \in \mathbb{F}$, we find that

$$d_r^2(x_a) = (-1)^{\tau(ar)}x_a, \quad q_r(x_a) = x_{a+r}.$$

For the chosen self-complementary basis $(b_1, \ldots, b_f)$, q_{b_j} commutes with $d_{b_k}^2$ if $j \neq k$ and the commutator of q_{b_j} and $d_{b_j}^2$ is $-\,\mathrm{id}$. From this we have:

Remark 17 *The group N_f is isomorphic to a central product of an extraspecial group $\langle q_{b_j}, d_{b_j}^2 \mid j = 1, \ldots, f\rangle \cong 2_+^{1+2f}$ with the center $Z(N_f) \cong \mathbb{Z}/4\mathbb{Z}$. The representation of N_f on the vector space $\oplus_{a\in\mathbb{F}}\mathbb{C}x_a$ of dimension 2^f is the unique irreducible representation of N_f such that $t \in \mathbb{Z}/4\mathbb{Z}$ acts as multiplication by i^t.*

Concerning the action of G_f on N_f we have

$$m_a d_r^2 m_a^{-1} = d_{a^{-1}r}^2, \quad m_a q_r m_a^{-1} = q_{ar}, \quad \text{for all } a, r \in \mathbb{F}^*.$$

Since m_a conjugates d_r to $d_{a^{-1}r}$ it suffices to calculate the action of d_1:

$$d_1 d_r^2 d_1^{-1} = d_r^2, \quad d_1 q_r d_1^{-1} = i^{\varphi(r)} q_r d_r^2, \quad \text{for all } r \in \mathbb{F}.$$

This proves

Lemma 18 *The image of the homomorphism $G_f \to \mathrm{Aut}(N_f/Z(N_f))$ is isomorphic to $\mathrm{SL}_2(\mathbb{F})$ via*

$$h \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad m_a \mapsto \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad d_1 \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Elementary calculations or explicit knowledge of the automorphism group of N_f (see [14]) show that the kernel of the above homomorphism is $N_f C_{G_f}(N_f) = N_f(G_f \cap \mathbb{C}^* \,\mathrm{id})$. It remains to find the center of G_f, which by the calculations above contains $i\,\mathrm{id}$. If f is even, then $\mathrm{cwe}(Q_4 \otimes_{\mathbb{F}_4} \mathbb{F})$ is an invariant of degree 4 of G_f, so the center is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ in this case. To prove the theorem, it remains to construct an element $\zeta_8\,\mathrm{id} \in G_f$ if f is odd, where $\zeta_8 \in \mathbb{C}^*$ is a primitive 8-th root of unity.

Lemma 19 *If f is odd, then $\langle (hd_1)^3 \rangle = \langle \zeta_8\,\mathrm{id}\rangle$.*

Proof. $(hd_1)^3$ acts trivially on $N_f/Z(N_f)$. Explicit calculation shows that $(hd_1)^3$ commutes with each generator of N_f, hence acts as a scalar. We find that

$$(hd_1)^3(x_0) = \frac{1}{\sqrt{|\mathbb{F}|}} \frac{1}{|\mathbb{F}|} \sum_{b,c\in\mathbb{F}} i^{\varphi(c+b)} (-1)^{\tau(c)} x_0.$$

The right hand side is an 8-th root of unity times x_0. If f is odd, then $\sqrt{2}$ is mentioned, which implies that this is a primitive 8-th root of unity. □

5 Extremal codes

Let $C \leq \mathbb{F}^n$ be a code. The complete weight enumerator $\mathrm{cwe}(C) \in \mathbb{C}[x_a \mid a \in \mathbb{F}]$ may be used to obtain information about the Hamming weight enumerator, which is the polynomial in a single variable x obtained from $\mathrm{cwe}(C)$ by substituting $x_0 \mapsto 1$ and $x_a \mapsto x$ for all $a \neq 0$.

Remark 20 *(a) If $\mathbb{F}' \leq \mathbb{F}$ is a subfield of $\mathbb{F}$ and $e = [\mathbb{F} : \mathbb{F}']$, then C becomes a code $C_{\mathbb{F}'}$ of length en over $\mathbb{F}'$ by identifying $\mathbb{F}$ with $\mathbb{F}'^e$ with respect to a self-complementary basis $(b_1, \ldots, b_e)$. If $a = \sum_{i=1}^{e} a_i b_i$ with $a_i \in \mathbb{F}'$, then the complete weight enumerator of $C_{\mathbb{F}'}$ is obtained from* $\mathrm{cwe}(C)$ *by replacing x_a by $\prod_{i=1}^{e} x_{a_i}$.*
(b) We may also construct a code C' of length n over $\mathbb{F}'$ from C by taking the $\mathbb{F}'$-rational points:

$$C' := \{c \in C \mid c_i \in \mathbb{F}' \text{ for all } i = 1, \ldots, n\}.$$

The dimension of C' is at most the dimension of C, and the complete weight enumerator of C' is found by the substitution $x_a \mapsto 0$ if $a \notin \mathbb{F}'$. C' is called the $\mathbb{F}'$-rational subcode of C.

As an application of Theorem 13 we have the following result. Note that the results for lengths $n \leq 20$ also follow from the classification of doubly-even self-dual codes in [4], [3] and [1], and the bound for length 20 can be deduced from [4, Cor. 3.4].

Theorem 21 *Let $\mathbb{F} := \mathbb{F}_4$. The maximal Hamming distance $d = d(C)$ of a doubly-even self-dual code $C \leq \mathbb{F}^n$ is as given in the following table:*

n	4	8	12	16	20	24
d	3	4	6	6	8	8

For $n = 4$ and 8, the quadratic-residue codes Q_4 resp. Q_8 are the unique codes C of length n with $d(C) = 3$ resp. $d(C) = 4$.

Proof. Let $p \in \mathbb{C}[x_0, x_1, x_\omega, x_{\omega^2}]_n^{G_2}$, a homogeneous polynomial of degree n. If p is the complete weight enumerator of a code C with $d(C) \geq d$, then the following conditions must be satisfied.

a) All coefficients in p are nonnegative integers.
b) The coefficients of $x_0^a x_1^b x_\omega^b x_{\omega^2}^b$ with $b > 0$ are divisible by 3.
c) $p(1, 1, 1, 1) = 2^n$.
d) $p(1, 1, 0, 0) = 2^m$ for some $m \leq \frac{n}{2}$.
e) $p(1, x, x, x) - 1$ is divisible by x^d.

One easily sees that Q_4 is the unique doubly-even self-dual code over $\mathbb{F}$ of length 4. If C is such a code of length 8 with $d(C) \geq 4$, then $\mathrm{cwe}(C)$ is uniquely determined by condition e). In particular the $\mathbb{F}_2$-rational subcode of C has dimension 4 and is a doubly-even self-dual binary code of length 8. Hence $C = \mathcal{H}_8 \otimes \mathbb{F} = Q_8$. If $C \leq \mathbb{F}^{12}$ is a doubly-even self-dual code with $d(C) \geq 6$, then again $\mathrm{cwe}(C) = \mathrm{cwe}(Q_{12})$ is uniquely determined by condition e), moreover Q_{12} has minimal distance 6.

For $n = 16$, there is a unique polynomial $p(x_0, x_1, x_\omega, x_{\omega^2}) \in \mathbb{C}[x_0, x_1, x_\omega, x_{\omega^2}]_{16}^{G_2}$ such that $p(1, x, x, x) \equiv 1 + ax^7 \pmod{x^8}$. This polynomial p has negative coefficients. Therefore the doubly-even self-dual codes $C \leq \mathbb{F}^{16}$ satisfy $d(C) \leq 6$. There are two candidates for polynomials p satisfying the five conditions above with $d = 6$. The rational subcode has either dimension 2 or 4 and all words $\neq 0, \mathbf{1}$ are of weight 8. One easily constructs such a code C from the code Q_{20}, by taking those elements of Q_{20} that have 0 in four fixed coordinates, omitting these 4 coordinates to get a code of length 16, adjoining the all-ones vector and then a vector of the form $(1^8, 0^8)$ from the dual code. $C_{\mathbb{F}_2} \leq \mathbb{F}_2^{32}$ is isomorphic to the extended binary quadratic-residue code and the rational subcode of C is 2-dimensional.

For $n = 20$ we similarly find four candidates for complete weight enumerators satisfying a) - e) above with $d = 8$ (where the dimension of the rational subcode is $1, 3, 5$ or 7). None of these satisfies e) with $d > 8$. The code Q_{20} has minimal weight 8 and its rational subcode is $\{\mathbf{0}, \mathbf{1}\}$. For $n = 24$, the code $Q_{24} = \mathbb{F}_4 \otimes \mathcal{G}_{24}$ has $d(C) = 8$. To see that this is best possible let $p \in \mathbb{C}[x_0, x_1, x_\omega, x_{\omega^2}]_{24}^{G_2}$ satisfy (b) and (e) above with $d = 9$. Then $p = p_0 + ah_1 + bh_2$, for suitable p_0, h_1, h_2 with $h_i(1, x, x, x) \equiv 0 \pmod{x^9}$, $p_0(1, x, x, x) \equiv 1 \pmod{x^9}$ and $a, b \in \mathbb{Z}$. Explicit calculations then show that $p_0(1, 1, 0, 0)$, $h_1(1, 1, 0, 0)$ and $h_2(1, 1, 0, 0)$ are all divisible by 3. Therefore $p(1, 1, 0, 0)$ is not a power of 2, hence p does not satisfy condition d). $\square$

Acknowledgment. We thank O. Jahn for computations in connection with Theorem 13 at an early stage of this work. We also thank the referees for their comments.

References

[1] K. Betsumiya, On the classification of Type II codes over $\mathbb{F}_{2^r}$ with binary length 32, preprint, 2002.

[2] K. Betsumiya and Y. J. Choie, Codes over $\mathbb{F}_4$, Jacobi forms and Hilbert-Siegel modular forms over $\mathbb{Q}(\sqrt{5})$, preprint, 2002.

[3] K. Betsumiya, T. A. Gulliver, M. Harada and A. Munemasa, On type II codes over $\mathbb{F}_4$, *IEEE Trans. Inform. Theory* **47**, (2001), 2242–2248.

[4] P. Gaborit, V. S. Pless, P. Solé and A. O. L. Atkin, Type II codes over $\mathbb{F}_4$, *Finite Fields Applic.* **8** (2002), 171-183.

[5] A. M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in *Actes, Congrés International de Mathématiques (Nice, 1970)*, Gauthiers-Villars, Paris, 1971, Vol. 3, pp. 211–215.

[6] M. Klemm, Eine Invarianzgruppe für die vollständige Gewichtsfunktion selbstdualer Codes, *Archiv Math.* **53** (1989), 332-336.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[8] G. Nebe, E. M. Rains and N. J. A. Sloane, The invariants of the Clifford groups, *Designs, Codes Cryptography* **24** (2001), 99–121.

[9] G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, book in preparation.

[10] G. Pasquier, Binary self-dual codes construction from self-dual codes over a Galois field $\mathbb{F}_{2^m}$, in *Combinatorial Mathematics (Luminy, 1981)*, ed. C. Berge et al., Annals Discrete Math. **17** (1983), 519–526.

[11] H.-G. Quebbemann, On even codes, *Discrete Math.* **98** (1991), 29–34.

[12] E. M. Rains and N. J. A. Sloane, *Self-dual codes* in *Handbook of Coding Theory*, ed. V. Pless and W. C. Huffman, Elsevier, Amsterdam, 1998, pp. 177–294.

[13] G. C. Shephard and J. A. Todd, Finite unitary reflection groups, *Canad. J. Math.* **6** (1954), 274-304.

[14] D. L. Winter, The automorphism group of an extraspecial p-group, *Rocky Mtn. J. Math.* **2** (1972), 159–168.

[15] J. Wolfmann, A class of doubly even self-dual binary codes, *Discrete Math.* **56** (1985), 299–303.